Last Time: Euclid's Algorithm for GCD

Bezout's Theorem.

Recall (Bezout's Theorem): If $a, b \in \mathbb{Z}$ not both 0, then there are $s, t \in \mathbb{Z}$ w/ $\boxed{\gcd(a,b) = as + bt.}$ ★

Also $\gcd(a,b) = \min\{n \in \mathbb{Z}_+ : n = as + bt \text{ for some } s, t \in \mathbb{Z}\}$.

Euclid's Extended Algorithm: ① Apply Euclid's Alg., remembering QRT applications. ② back-sub to get the desired linear combination.

Ex: Compute $s, t \in \mathbb{Z}$ w/ $\gcd(99, -900) = 99s + (-900)t$.

Sol: Applying Euclid's Algorithm:

$$900 = 99 \cdot 9 + 9 \qquad \therefore \quad 9 = \gcd(99, 900) = 99(-9) + 900(1)$$
$$99 = 9 \cdot 11 + 0 \qquad = 99(-9) + (-900)(-1). \quad \blacksquare$$

Application: Solving equations modulo m...

Defn: Let $m \in \mathbb{Z}_+$ and suppose $a \in \mathbb{Z}/m\mathbb{Z}$.
a is a unit mod m when there is $b \in \mathbb{Z}/m\mathbb{Z}$ such that $ab \equiv 1 \bmod m$.

Interpretation: In the cayley table for $\cdot$ mod m, we have $[a][b] = [1]$. So we can think of "$[b] = 1/[a]$": We will write $[b]_m = [a]_m^{-1}$.

Prop: Let $a, m \in \mathbb{Z}$ w/ $m > 0$. The following are equivalent:

① a is a unit mod m.

② there is $b \in \mathbb{Z}$ w/ $ab \equiv 1 \bmod m$.

③ Every linear equation $ax + c \equiv 0 \bmod m$ has a solution mod m (i.e. such an x exists).

④ $\gcd(a, m) = 1$ (i.e. a is relatively prime to m).

NB: If $\gcd(a,b) = 1$ (for $a, b \in \mathbb{Z}_+$), we say a is relatively prime to b.

pf: Let $a, m \in \mathbb{Z}$ w/ $m > 0$.

①↔②: This is the definition of "unit mod m".

②→③: Suppose there is a $b \in \mathbb{Z}$ w/ $ab \equiv 1 \bmod m$.

Letting $x = b(-c)$, we see $x \in \mathbb{Z}$ by closure and

$$\begin{aligned} ax + c &= a(b(-c)) + c \\ &= (ab)(-c) + c \\ &\equiv 1(-c) + c \\ &= -c + c = 0 \bmod m, \end{aligned}$$

so $ax + c \equiv 0 \bmod m$, as desired.

③→④: Suppose every equation of the form $ax + c \equiv 0 \bmod m$ has a solution in $\mathbb{Z}$.

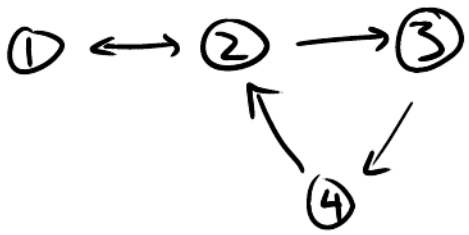
If $c = 1$, we seek to solve $ax + 1 \equiv 0 \bmod m$. This has solution $s \in \mathbb{Z}$; i.e. $as + 1 \equiv 0 \bmod m$.

Thus $m \mid (as + 1 - 0)$ by a previous proposition. Thus $as + 1 = mt$ for some $t \in \mathbb{Z}$. Rearranging, we obtain $1 = a(-s) + mt$. Thus, by Bezout's Theorem $1 = \gcd(a, m)$ as desired.

④ → ②: Suppose $\gcd(a, m) = 1$. By Bezout's Theorem, $ab + mt = 1$ for some $b, t \in \mathbb{Z}$. Reducing mod m: $1 = ab + mt \equiv ab + 0 \cdot t = ab \pmod m$.

Hence $ab \equiv 1 \pmod m$ for some $b \in \mathbb{Z}$, as desired.

Hence, we showed the following chain of implications:



Hence, the original statement holds ☑

Ex: Solve $15x \equiv 7 \pmod{49}$.

Sol: First we compute $\gcd(15, 49)$:

$$49 = 15 \cdot 3 + 4$$
$$15 = 4 \cdot 3 + 3$$
$$4 = 3 \cdot 1 + 1$$
$$3 = 1 \cdot 3 + 0$$

Next apply back substitution:

$$1 = 4 - 3 \cdot 1 = 4 \cdot 1 + 3(-1)$$
$$= 4 \cdot 1 + (15 - 4 \cdot 3)(-1) = 4(1) + 15(-1) + 4(3)$$
$$= 4(4) + 15(-1) = (49 - 15(3))(4) + 15(-1)$$
$$= 49(4) + 15(-12) + 15(-1)$$
$$= 15(-13) + 49(4)$$

Hence -13 is an inverse of 15 mod 49

i.e. $-13 \equiv 49 - 13 = 36 \pmod{49}$, so 36 is the desired inverse. To finish solving the equation:

$$x \equiv 36(15x) \equiv 36 \cdot 7 = 252 \equiv 252 - 49(5) = 7 \pmod{49}.$$ ☑

NB: Started late and ended early because campus WiFi is bad.